



22883

PATENT TRADEMARK OFFICE

103.1019.10

## IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

DAVID HITZ et al.

Serial No.: N/Y/A (continuation of  
parent application serial  
no. 09/035,234)Filed: Herewith (parent  
filed Mar. 3, 1998)For: FILE ACCESS CONTROL IN A  
MULTI-PROTOCOL FILE SERVER

Art Unit: N/Y/A (parent: 2184)

Examiner: N/Y/A (parent: NADEEM IQBAL)

Tel: N/Y/A (parent: (703) 308-5228)

Office Action Mailed:

N/Y/A (parent: Office Action  
mailed Apr. 10, 2001)CERTIFICATE OF MAILING (37 CFR § 1.8)I hereby certify that this correspondence is being  
deposited with the United States Postal Service with  
sufficient postage as First Class Mail, in an envelope  
addressed to:Assistant Commissioner for Patents  
Washington, DC 20231on 8-10-01 *Delette M. Marks*  
Date By:Honorable Assistant Commissioner  
for Patents  
Washington, D.C. 20231PRELIMINARY AMENDMENT

Dear Sir:

This is a preliminary amendment for a continuation application filed herewith  
under 37 C.F.R. § 1.53(b) of application serial no. 09/035,234 filed Mar. 3, 1998.

Prior to examination, please amend the above-identified application as follows.

IN THE SPECIFICATION:

Page 1, line 16, please insert the following paragraph:

-- This application is a continuation of application serial no. 09/035,234 filed Mar.  
3, 1998.--

IN THE CLAIMS:

Please amend the claims such that the pending claims read as follows:

31. (New) A method of operating a file server, said method including steps of:  
identifying a first file on said file server with a first security style selected from  
among a plurality of security styles corresponding to a plurality of operating systems  
implemented on said file server; and  
enforcing said first security style for all accesses to said first file.

32. (New) A method as in claim 31, wherein said plurality of security styles  
includes a Windows NT security style.

33. (New) A method as in claim 31, wherein said plurality of security styles includes a Unix security style.

34. (New) A method as in claim 31, wherein said enforcing step enforces said security style for all accesses to the first file regardless of the security style associated with the entity who seeks access to the first file.

35. (New) A method as in claim 31, including the steps of:  
associating said first file with a subset of files in a file system; and  
limiting said subset of files to a security subset of said plurality of security style;  
wherein attempts to set permission in said subset of files are restricted to said security subset.

36. (New) A method as in claim 35, wherein said security subset includes a Windows NT security style.

37. (New) A method as in claim 35, wherein said security subset includes a Unix security style.

38. (New) A method as in claim 35, further comprising the step of caching associations and limits for the subset of files for future use.

39. (New) A method as in claim 35, wherein the steps of associating and limiting can be performed dynamically, associated with a specific attempt to access a file, or statically, not associated with a user or specific attempt to access a file.

40. (New) A method of operating a file server, said method including steps of identifying a first file on said file server with a first security style selected from among a plurality of security styles corresponding to a plurality of operating systems implemented on said file server;

enforcing said first security style for all accesses to said file server; and

identifying said first file with a second security style selected from among the plurality of security styles in response to a file server request.

41. (New) A method as in claim 40, including steps of associating said second security style with a file server request for setting permissions for said first file when said file server request is successful.

42. (New) A method as in claim 40, wherein said first file is associated with said second security style regardless of the security style previously associated with said first file.

43. (New) A file server including:

a set of files available on said file server, each said file having an associated security style selected from among a plurality of security styles corresponding to a plurality of operating systems implemented on said file server;

wherein said file server enforces said associated security style for all accesses to said file.

44. (New) A file server as in claim 43, wherein said plurality of security styles includes a Windows NT security style.

45. (New) A file server as in claim 43, wherein said plurality of security styles includes a Unix security style.

46. (New) A file server as in claim 43, including  
a subtree of files in said file system associated with a security subset of said plurality of security styles;  
wherein said file server restricts attempts to set permissions in said subtree to said security subset.

47. (New) A file server as in claim 46, wherein said security subset includes a Windows NT security style.

48. (New) A file server as in claim 46, wherein said security subset includes a Unix security style.

49. (New) A file server as in claim 43, wherein said file server is capable of altering the security style associated with said file in response to a file server request.

50. (New) A file server as in claim 69, wherein said file server is capable of altering the security style associated with said file in response to a file server request when said file server request is successful.

51. (New) In a file server having a plurality of files, a data structure associating a security style with each said file, said security style being selected from among a plurality of security styles corresponding to a plurality of operating systems implemented on said file server.

52. (New) A data structure as in claim 51, wherein said plurality of security styles includes a Windows NT security style.

53. (New) A data structure as in claim 51, wherein said plurality of security styles includes a Unix security style.

54. (New) In a file server having a plurality of files and a security style associated with each file, said security style being selected from among a plurality of security styles corresponding to a plurality of operating systems implemented on said file server, a data structure associating a security subset of said plurality of security styles with a subtree of said files available on said file server.

55. (New) A data structure as in claim 54, wherein said security subset includes a Windows NT security style.

56. (New) A data structure as in claim 54, wherein said security subset includes a Unix security style.

REMARKS:

New claims 31 to 56 are in the application. Claims 31, 40, 43 and 51 are the independent claims herein. Examination and early passage to issue are respectfully requested.

Claim Correspondence and Changes

Claims 31 to 56 correspond to claims rejected in an Office Action mailed Apr. 10, 2001, in the parent and subsequently cancelled from the parent. Claims 31 to 39 correspond to claims 42 to 50 from the parent, claims 40 to 42 correspond to claims 57 to 79 from the parent,

claims 43 to 50 correspond to claims 63 to 70 from the parent, and claims 51 to 56 correspond to claims 72 to 77 from the parent.

Claim 49, which corresponds to claim 69 from the parent, has been amended into dependent form. Claim 40, which corresponds to claim 57 from the parent, has been amended to recite that the plurality of operating systems are implemented on the recited file server. Several additional changes have been made to correct minor informalities.

Furthermore, "steps for" terminology has been replaced with "steps of" terminology in the method claims, thereby emphasizing that these claims are not within the ambit of 35 U.S.C. 112, paragraph 6. These changes have not been made for reasons related to patentability.

#### Claim Rejections in Parent

The claims in the parent corresponding the pending claims herein were all rejected under 35 U.S.C. 103(a) over U.S. Patent No. 5,675,782 (Montague). Applicants respectfully submit that a rejection of the pending claims under section 103(a) over Montague would not be proper for at least the following reasons.

Claim 31 recites a method of operating a file server. The method includes steps of identifying a first file on the file server with a first security style selected from among a plurality of security styles corresponding to a plurality of operating systems implemented on the file server, and enforcing the first security style for all accesses to the first file.



Claim 40 also recites a method of operating a file server. The method of claim 40 includes the steps of identifying a first file on the file server with a first security style selected from among a plurality of security styles corresponding to a plurality of operating systems implemented on the file server, enforcing the first security style for all accesses to the file server, and identifying the first file with a second security style selected from among the plurality of security styles in response to a file server request.

Claim 43 recites a file server including a set of files available on the file server, each file having an associated security style selected from among a plurality of security styles corresponding to a plurality of operating systems implemented on the file server. According to claim 43, the file server enforces the associated security style for all accesses to the file.

Claim 51 recites a data structure in a file server having a plurality of files. The data structure of claim 51 associates a security style with each file, the security style being selected from among a plurality of security styles corresponding to a plurality of operating systems implemented on the file server.

Each of these independent claims involves and recites a security style selected from among a plurality of security styles corresponding to a plurality of operating systems implemented on a file server. Montague simply is not seen to be concerned with such file servers that implement a plurality of operating systems.

In more detail, as recited in its Abstract, Montague concerns "controlling access to entities on a network on which a plurality of servers are installed that use different operating

systems." Plural servers using different operating systems is different from a server that implements plural operating systems (and hence security styles).

The closest that Montague is seen to come to discussing a single server that implements a plurality of operating systems is at column 6, line 65, to column 7, line 2, which discusses block 50 of Figure 2. This block is labeled "Other Operating Systems – If Applicable." A close reading of column 6, line 65, to column 7, line 2, reveals that this block is merely meant to be a "catch-all" to cover operating systems not specifically named by Montague. The rest of Montague simply is not seen to discuss or address operation of a server that implements plural operating systems and corresponding security styles.

The fact that Montague does not discuss a server that implements plural operating systems flows from the focus of Montague's disclosure. A careful reading of Montague's Background of the Invention reveals that Montague is concerned with controlling access to objects on different servers, each of which is running a different operating system. The invention, in contrast, is concerned with controlling access and permissions for objects implemented on a file server using different security styles corresponding to different operating systems implemented on that server.

In short, Montague is understood to concern multiple servers that each implement a possibly different operating system. The invention concerns a file server that itself implements multiple operating systems and corresponding security styles.

The foregoing discrepancy between Montague and the invention was not addressed by the Apr. 2001 Office Action in the parent. In particular, the rejection of claim 42 in

the parent (now claim 31) at page 3 of the Office Action alleged that Montague taught "identifying a first file on the file server with a first security style selected from among a plurality of security styles." However, this rejection apparently ignored claim 42's (now claim 31's) limitation that the plurality of security styles correspond to a plurality of operating systems implemented on the file server.

The Apr. 2001 Office Action was likewise deficient in its rejections of claims 63 and 72 in the parent (now claims 43 and 51). While claim 57 in the parent (now claim 40) did not recite that the plurality of security styles correspond to a plurality of operating systems implemented on a file server, that claim has been amended herein to recite this limitation.

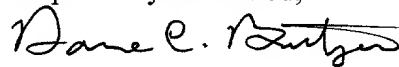
Thus, Applicants respectfully submit that the now-pending claims clearly are not obvious over Montague under 35 U.S.C. 103(a).

Closing

In view of the foregoing, the entire application is believed to be in condition for allowance, and such action is respectfully requested at the Examiner's earliest convenience.

Applicants' undersigned attorney can be reached at (614) 486-3585. All correspondence should continue to be directed to the address indicated below.

Respectfully submitted,



Dane C. Butzer  
Reg. No. 43,521

Dated: July 12, 2001  
The Swernofsky Law Group  
P.O. Box 390013  
Mountain View, CA 94039-0013  
(650) 947-0700

103.1019.10

Changes to Specification

Pursuant to 37 C.F.R. § 1.121(b)(iii), changes to the specification effected by the accompanying paper are indicated below.

Page 1, line 16, the following paragraph has been inserted:

-- This application is a continuation of application serial no. 09/035,234 filed Mar.  
3, 1998.--

Changes to Claims

Pursuant to 37 C.F.R. § 1.121(c)(ii), changes to any claims effected by the accompanying paper are indicated below.

Claims 1 to 30 have been cancelled without prejudice or disclaimer of subject matter.

Claims 31 to 56 have been added.